(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2001 (20.12.2001)

PCT

(10) International Publication Number
WO 01/97439 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US00/33864

(22) International Filing Date:
14 December 2000 (14.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/593,893 14 June 2000 (14.06.2000) US

(71) Applicant: COMMERCIAL ELECTRONICS LLC [—/US]; 375 Park Avenue, Suite 1604, New York, NY 10152 (US).

(72) Inventors: PADGETT, Robert, D.; 35 Nutmeg Drive, Trumbull, CT 06611 (US). MAXWELL, John, C., III; Commercial Electronics, LLC, Suite 1604, 375 Park Avenue, New York, NY 10152 (US).

(74) Agent: LIEB, Stephen, J.; Orrick, Herrington & Sutcliffe LLP, 666 Fifth Avenue, New York, NY 10103 (US).

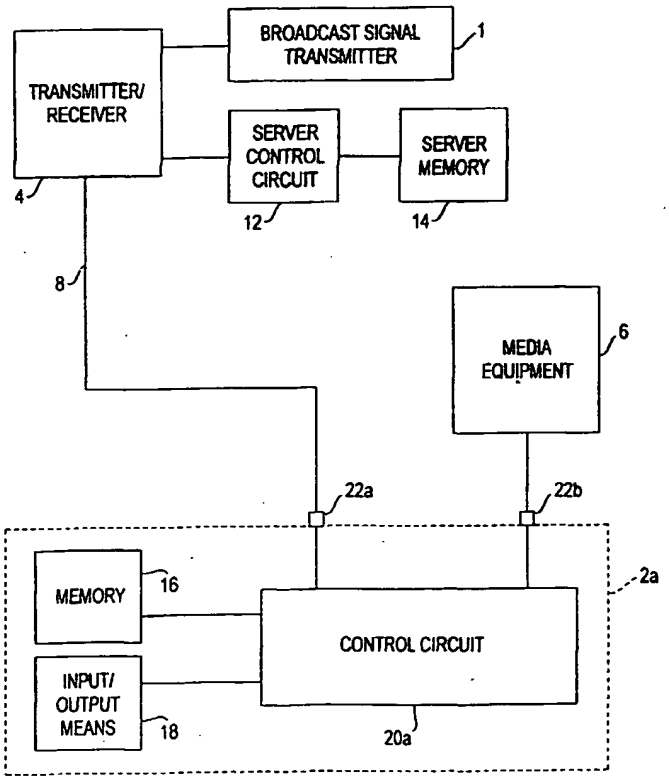
(81) Designated States *(national)*: CA, IL, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A METHOD AND SYSTEM FOR VIEWER IDENTIFICATION AND DATA COLLECTION VERIFICATION



(57) Abstract: A method and system for viewer identification and data collection verification which ensures the identity of the viewer submission of collected data (220) regarding a broadcast. The viewer is given a unique identifier (174) which can be a personal identification number or digitized biological indicia. The unique identifier is used to positively identify a viewer and to encode (180) any data transmitted between a viewer and a survey company.

WO 01/97439 A1

A Method and System for Viewer Identification and Data Collection Verification

FIELD OF THE INVENTION

The present invention relates to the field of verification and authentication of marketing surveys, more specifically, the present invention relates to the use of personal identification numbers and cryptography to identify viewers and verify data regarding selection of broadcasted signals by a viewer.

BACKGROUND OF THE INVENTION

Proper marketing of broadcasted products, such as television shows, radio shows, and computer network programs, requires feedback from viewers of the broadcasts. The data, which is required to analyze a viewing audience, is extensive. Not only is broadcast selection, time spent viewing a selection, and the number of people viewing the selection important, but the biographic and demographic information of the viewers is important. Market analysts require information such as age, gender, education, income, marital status, and ethnicity to develop marketing schemes directed at specific targeted groups. Because the industry is so competitive and the number of viewers are typically very large, the manner in which data is collected must be accurate and efficient.

Typically, survey companies collect the data and prepare reports which are then distributed to interested media companies. According to the typical method, the data is collected by viewers who keep track of their selections in written form. The written record is then sent to the survey company to compile and organize the data. The human error involved in recording broadcast selections and reporting the data to the survey company makes the method inaccurate.

Further, the viewer is burdened by the preparation of lists and submission of those lists to the survey company. In addition, the time necessary to gather and organize data entered on paper makes this method inefficient.

More recently, survey companies have installed viewer boxes, which are connected to media equipment (e.g., television, radio, computer). As the viewer watches a selected broadcast, the viewer box records the relevant information (e.g., channel, time spent on channel). This information is then transmitted to the survey company by some electronic means known in the art. The viewer is relieved of the burden of keeping and submitting lists of selections by this method, but an inaccuracy still remains because the viewer box is passive with regard to identifying the viewer. Typically, the viewer box includes a means for individual viewers to indicate that they are viewing a broadcast selection by pressing one of a plurality of buttons on the viewer box. The button is specifically assigned to that viewer. Since anyone can press the button, however, erroneous identification of which viewer is watching a given selection is possible. The data collected from a viewer box could be associated with a viewer, which is different from the actual viewer. The result is an inaccurate collection of data.

A third method, which actively detects the number of viewers, has also been utilized by survey companies. The active method uses ultrasonic wave maps to map a viewing area when it is empty and when it is occupied with viewers. The first collected map, which is of the empty viewing area, is subtracted from the second collected map, which is of the occupied viewing area. The resulting map is processed to determine the number of viewers in an audience. This method is flawed because it cannot discriminate between viewers. A total number of viewers in a viewing area may be approximated by this method, but the viewer's identity cannot be

discerned. An unidentified viewer may be present or viewers having known identities may be confused. Therefore, inaccurate data collection may still result.

A fourth method requires that each viewer wear a transmitter, which transmits an identification signal identifying that individual viewer. At predetermined periods, the transmitter transmits the identification signal to a receiver box. The receiver box records the identified viewer as viewing a particular broadcast. The same problems are associated with this method as with the other methods. The transmitter may be left in the viewing area when the viewer leaves or the transmitter may be worn by another individual. This results in the inaccurate collection of data. Further, wearing a transmitter is inconvenient and there is a high likelihood that the viewer will take it off, further reducing the accuracy of the results.

The present invention solves the problems associated with the prior art discussed above.

BRIEF SUMMARY OF THE INVENTION

An advantage of the present invention is that it provides a method and system to identify a viewer of a selected broadcast signal.

A further advantage of the present invention is that it provides a method and system which uses a unique identifier to identify a viewer of a selected broadcast signal.

A further advantage of the present invention is that it provides a system which uses a bio-signature to identify a viewer of a selected broadcast signal.

A further advantage of the present invention is that it provides a method and system to verify the data collected regarding broadcast signal selections made by a viewer.

An even further advantage of the present invention is that it provides a method and system which uses a personal identification number and cryptography to verify the identity of a viewer and data collected regarding broadcast signal selections made by the viewer.

Broadly, the present invention is directed to a method and system for viewer identification and data collection verification that confirms the identity of the viewer before submission of collected data regarding a broadcast. The viewer is assigned a first unique identifier which can be a personal identification number or digitized biological indicia. The first unique identifier is used to positively identify a viewer and to encode any data transmitted between a viewer and a survey company, thereby confirming positive identification of the data also. Encoding the data also provides a secure means to transmit the data to prevent unauthorized use of that data. The data is also encoded using a cryptographic key. Accordingly, the cryptographic key is part of a public key/private key pair. The two layers of encoding provide additional security.

Operationally, an apparatus according to the present invention transmits identical mobile agents including the first unique identifier and public key/private key pair simultaneously to a broadcast audience that may include millions of viewers. The mobile agent will only be activated at a viewer's location if the viewer enters a second unique identifier which matches the first unique identifier. The remaining mobile agents transmitted to locations other than the viewer's location of the viewer assigned the first unique identifier (i.e., the mobile agents in which a second unique identifier does match the first unique identifier) are transmitted back to

the survey company accompanied by an error message indicating that the viewer did not enter the correct second unique identifier. Once the mobile agent is activated, it begins collecting data, such as the television channel being watched and the time spent watching that channel. After a predetermined time period, the collected data is sent to the survey company along with the first unique identifier. The first unique identifier is included with the collected data so that the viewer is correctly identified. A table of definitions including the above terms is provided at the end of the Detailed Description of the Invention

In accordance with one form of the invention, a first unique identifier is assigned to a viewer and stored in a memory in a server. The first unique identifier can be assigned by selecting a unique alphanumeric sequence of a predetermined length from a list of unused alphanumeric sequences and assigning the unique alphanumeric sequence to the viewer. The assignment is then recorded in the server memory and the unique alphanumeric sequence is removed from the list of unused alphanumeric sequences. Alternatively, the first unique identifier can be assigned by creating a digital representation of a body characteristic of a viewer and associating that digital representation to the viewer. The assignment is then stored in the server memory.

A public/private key pair is then generated and the first unique identifier is encrypted using the public key, which forms an encrypted unique identifier. The public key is then stored in the server memory. The public/private key pair is appended to a mobile agent, which forms a keyed mobile agent. The mobile agent is computer code, which includes a set of commands, which can be executed by a viewer box and can also include biographic and demographic data regarding a specific viewer. The set of commands includes instructions to the viewer box on what data to collect and for what period of time to collect the data. The keyed mobile agent is

encrypted using the first unique identifier, which forms an encrypted keyed mobile agent. The encrypted unique identifier is appended to the encrypted keyed mobile agent, which forms a unique encrypted keyed mobile agent.

The unique encrypted keyed mobile agent is then transferred from the server to the viewer box and the viewer enters a second unique identifier in the viewer box. The encrypted keyed mobile agent is separated from the unique encrypted keyed mobile agent and is decrypted using the second unique identifier, thereby forming a decrypted keyed mobile agent. The private key is then separated from the mobile agent in the decrypted keyed mobile agent and the encrypted unique identifier is decrypted using the private key, which forms a data string. The data string and the second unique identifier are compared. If they are identical, the mobile agent is stored in memory at the viewer box. The data string is identical to the second unique identifier if the second unique identifier is identical to the first unique identifier. If the second unique identifier is different from the first unique identifier, the data string will not match the second unique identifier.

If the data string and the second unique identifier match, the mobile agent is activated and a plurality of broadcast signals are received by the viewer box. Under the instructions from the mobile agent, the viewer box then records in a memory which broadcast signal is selected and for how long each broadcast selection is viewed. A data agent is then formed by appending the collected data to the mobile agent forming a data agent and the data agent is encrypted using the private key to form an encrypted data agent. The second unique identifier is then appended to the encrypted data agent to form a unique encrypted data agent. The unique encrypted data agent is transferred to the server where it is registered by comparing the unique identifiers in the server memory with the appended second unique identifier. Once a matching unique identifier is

found, the corresponding private key is retrieved from the server memory and the encrypted data agent is decrypted using the private key, which forms a decrypted data agent. The collected data and mobile agent are stored in the server memory.

The private key may be appended to the mobile agent by creating a digital word with the mobile agent and placing the private key in front of the digital word in a data stream. A marker is then placed in front of the private key in the data stream. The marker indicates the starting positions of the private key and mobile agent in the data stream.

The step of requesting a second unique identifier from the viewer is accomplished, according to one embodiment of the invention, by first determining that the unique encrypted keyed mobile agent has been received at the second location and then outputting a message to the viewer to enter the second unique identifier. The message to the viewer requesting entry of the second unique identifier can be made by displaying a message on a display means, illuminating an indicator light, or generating an audio signal. In response to the request, the viewer can enter the second unique identifier by entering a personal identification number on a keypad or other user interface (e.g., scanning a bar code in a reader) which is in communication with a viewer box or by inputting the digitized unique biological identifier. According to another embodiment of the invention, instead of signaling the user to enter the second unique identifier, the viewer box does not activate until a unique identifier is entered. This would prevent viewing of the broadcast signal until the viewer has identified himself to the viewer box.

The viewer can input a digitized unique biological identifier by inserting an appendage, for example, the tip of a finger, into a print reader which scans the appendage and creates a digital representation of the appendage's print which is then input into the viewer box.

Alternatively, the viewer can input a digitized unique biological identifier by placing his eye near a retinal scanner which scans the viewer's retina and creates a digital representation of the viewer's retina. The digital representation of the retinal scan is then input to the viewer box.

Separating the encrypted keyed mobile agent from the unique encrypted keyed mobile agent is accomplished, according to one embodiment of the invention, by locating a marker in a data stream which contains the unique encrypted keyed mobile agent and reading the marker to determine the starting position of each piece of data in the encrypted keyed mobile agent. Once the starting positions are known, the first unique identifier, private key, public key, and mobile agent are separated into individual digital words. The individual digital words, according to one embodiment of the invention, are sixteen bits long and are arranged in data fields in serial order as follows: (1) first unique identifier; (2) private key; (3) public key; and (4) mobile agent. According to another embodiment, each data field is a plurality of sixteen-bit words. Data collection at the second location is accomplished by determining the broadcast channel selected by the viewer and recording the selected broadcast channel and the elapsed time viewing the selected broadcast channel in a memory at the second location.

According to one embodiment of the invention, a viewer changes a selected broadcast channel by first entering a unique identifier (e.g., PIN, thumbprint, retinal scan) and then changing the channel. The viewer box will then be able to track exactly what broadcast channel was selected and for how long a particular viewer watched the selected broadcast channel. According to another embodiment, a remote control includes a keypad wherein selected keys of the keypad scan the print of a finger as the key is pressed. The print reading keys allow a viewer to select broadcast channels in one step (i.e., without separately entering the unique identifier).

Another aspect of the present invention allows a public key/private key pair to be securely transferred to a viewer box. To accomplish the secure transfer, a first unique identifier is assigned to a viewer and stored in a memory by a server using the methods described above. A public/private key pair is then generated by the server and the first unique identifier is encrypted using the private key to form an encrypted unique identifier. The public key and private key are then stored in the memory. The public key and private key are then encrypted using the first unique identifier to form encrypted keys. The encrypted unique identifier is appended to the encrypted keys forming unique encrypted keys. The unique encrypted keys are then transferred from the server to the viewer box.

A second unique identifier is then requested from the viewer by the viewer box. In response, the viewer enters the second unique identifier that was previously assigned. According to one embodiment of the invention, the first and second unique identifiers are identical. The encrypted keys are then separated from the unique encrypted keys and the encrypted keys are decrypted using the second unique identifier to form a decrypted private key and decrypted public key. The encrypted unique identifier is then decrypted using the private key form a data string. The data string and the second unique identifier are then compared. If the data string and the second unique identifier are identical, the decrypted keys are stored in memory in the viewer box. If they are not identical, an error message is returned to the server.

Another aspect of the invention is directed to a secure method for collecting viewer data that does not use cryptography. According to one embodiment, a first unique identifier is assigned to a viewer and the first unique identifier is stored in a memory in the server. The first unique identifier is then appended to a mobile agent to form a unique mobile agent. The mobile agent includes a set of commands. The unique mobile agent is then transmitted to a viewer box.

The viewer box is attached to media equipment. The unique mobile agent is then registered by the viewer box by comparing the first unique identifier transmitted from the server with a second unique identifier entered into the viewer box by the viewer. After registering the unique mobile agent, a viewer chooses from a plurality of broadcast signals, which are received by the viewer box. The selection of a broadcast signal is recorded in memory in the viewer box as collected data. The unique identifier is then appended to the collected data to form unique collected data and the unique collected data is transmitted back to the server. The unique collected data is then registered by the server and the collected data is stored in a memory in the server.

The viewer box for one embodiment of a system for viewer identification and verification of collected data connected to a media device according to the present invention includes a control circuit, a memory circuit electrically connected to the control circuit, an input means electrically connected to the control circuit, and an output means electrically connected to the control circuit. The control circuit has a means to determine which broadcast signal is selected by a viewer. The memory circuit stores any data collected by the control circuit and any instruction set carried out by the control circuit. The input means allows the viewer to enter data into the control circuit and the output means allows the control circuit to prompt a viewer to enter information into the input means.

According to one embodiment of the invention, the control circuit includes one of a variety of communications configurations. The first configuration includes a two-way communication port connected between the control circuit and a transmitter/receiver and a one-way or two-way communication port connected between the control circuit and media equipment. The second configuration includes a one-way or two-way communication port connected between the control circuit and a transmitter/receiver, a one-way or two-way communication port connected between the control circuit and media equipment, and a two-way

communication port connected between the control circuit and a server circuit. The third configuration includes a low power atmospheric transmitter/receiver, a low power atmospheric transmitter/receiver controller, a two-way low power atmospheric transmitter/receiver port, and a one-way or two-way communication port connected between the control circuit and media equipment. These configurations are disclosed by way of example. Other configurations can be used and remain within the scope of the invention.

According to a further embodiment of the invention, a system for viewer identification and verification of collected data includes a transmitter, a viewer box, a server circuit, a receiver connected between the viewer box and a server circuit, and media equipment. The transmitter transmits a combined signal including a broadcast signal and a mobile agent signal to the viewer box. The viewer box receives the combined signal and is capable of transmitting a data signal. The server circuit includes a server control circuit and a server memory. The receiver receives the data signal which is transmitted from the viewer box and couples the signal to the server circuit. The media equipment is responsive to the transmitter and displays the broadcast signal transmitted by the transmitter.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects, features, and advantages of the present invention will be apparent from the following detailed description of the invention, which is to be read in connection with the accompanying drawings, in which like reference characters refer to like elements, and in which:

Figure 1 is a functional diagram of a system for viewer identification and data collection verification formed in accordance with a first embodiment of the present invention;

Figure 2 is a functional diagram of a system for viewer identification and data collection verification formed in accordance with a second embodiment of the present invention;

Figure 3 is a diagram of a flowchart illustrating the steps of a method for viewer identification and data collection formed in accordance with the first embodiment of the present invention;

Figure 4 is a diagram of a flowchart illustrating the steps of a method for viewer identification and data collection verification formed in accordance with the second embodiment of the present invention; and

Figure 5 is a diagram of a flowchart illustrating the steps of a method for securely transferring a public key/private key pair to a remote location for use in a viewer identification and data collection verification system formed in accordance with a further embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 is a functional diagram of a system for viewer identification and data collection verification according to a first embodiment of the invention. A viewer box 2a is placed in proximity to a viewer's media equipment 6 (e.g., television, radio, personal computer). The viewer box 2a includes a control circuit 20a, an input/output ("I/O") means 18, and memory 16. The control circuit 20a is connected to a first I/O port 22a and a second I/O port 22b to which electrical connections can be made. The I/O ports 22a, 22b are merely modular connectors which are well known in the art of electrical connections. The viewer box 2a (or 2b, which is shown in Figure 2) may have its own power supply or, preferably, will draw power from the

media equipment 6 or a local receiver 24 (shown in Figure 2) as is well known in the art. A transmitter/receiver 4 is electrically connected to a broadcast signal transmitter 1 and a server control circuit 12. The broadcast signal transmitter 1 (e.g., television transmitter, radio transmitter) is well known in the art and transmits a broadcast signal to the transmitter/receiver 4. The server control circuit 12 is connected to a server memory 14. The server memory 14 is a memory circuit that is accessed and controlled by the server control circuit 12 and is a type of memory circuitry known in the art. The server control circuit 12 transmits a mobile agent signal to the transmitter/receiver 4. The mobile agent signal includes a set of instructions to be carried out by a control circuit 20a. The mobile agent may also include biographic or demographic information regarding the specific viewer for which it is generated.

The transmitter/receiver 4 combines the broadcast signal and mobile agent signal using means known in the art (e.g., frequency multiplexing). The combined signal is then transmitted via connection 8 to the first I/O port 22a. The server control circuit 12 transmits a mobile agent signal periodically. When server control circuit 12 is not transmitting a mobile agent signal, the transmitter/receiver 4 transmits the broadcast signal to the first I/O port 22a. The first I/O port 22a receives the combined signal or the broadcast signal when the server circuit is not transmitting a mobile agent signal. According to one embodiment of the invention, the connection 8 between the transmitter/receiver 4 and the I/O port 22a is a physical connection, such as coaxial cable, telephone line, or fiber optic cable. According to a further embodiment, the connection 8 is a two-way fiber optic cable that carries both the broadcast signal and mobile agent signal. According to an alternative embodiment, the connection 8 is a radio or microwave frequency signal and the viewer box includes means for receiving such signals.

Internally in the viewer box 2a, the control circuit 20a is connected to the I/O means 18 and memory 16. The connections are two-way, allowing signals to be transmitted and received between the control circuit 20a and either memory 16 or the I/O means 18. The control circuit 20a controls the operation of memory 16 and the I/O means 18. The input/output means 18 may include any one of several input/output means. As input means, input/output means 18 may include a keypad, print reader (e.g., fingerprint, footprint), retinal scanner, infrared receiver, or other data input means adapted to receive identifying information from a viewer. According to one embodiment of the invention, the input means is a print reader. The output means includes a light emitting diode, infrared transmitter, speaker, or display of a kind known in the art. Memory 16 is memory circuitry known in the art including magnetic or optical disk drives, solid state memory devices, and the like. The control circuit 20a is connected to the second I/O port 22b. The second I/O port 22b is connected to the media equipment 6. The control circuit 20a is capable of determining which broadcast signal is selected by the viewer and includes an internal clock.

In operation, the broadcast signal transmitter 1 continuously transmits a broadcast signal to the transmitter/receiver 4. The server control circuit 12 transmits signals including mobile agents intermittently when mobile agents need to be transmitted. When the server control circuit 12 transmits a mobile agent signal, the broadcast signal and mobile agent signal are combined by the transmitter/receiver 4 into one signal which is transmitted to the viewer box 2a.

In the viewer box 2a, the combined signal is coupled to the control circuit 20a where the combined signal is separated into the broadcast signal and the mobile agent signal. This can be accomplished by frequency filtering the combined signal or by other means known in the art to separate multiple signals. The broadcast signal is coupled through the control circuit 20a to the

second I/O port 22b and then to the media equipment 6, where it is presented to the viewer. The media equipment 6 includes televisions, radios, personal computers, and the like. The media equipment 6 is responsive to the signal emitted from second I/O port 22b of the viewer box 2a.

Upon receipt of a mobile agent signal, the control circuit 20a registers the signal. The first step in registering the mobile agent is to request that the viewer enter a second unique identifier into the I/O means 18. The control circuit 20a instructs I/O means 18 to request entry of the second unique identifier by the viewer. According to one embodiment, the I/O means 18 makes the request by generating characters which are coupled through the control circuit 20a and displayed on the media equipment 6. According to another embodiment, the I/O means illuminates a light emitting diode. According to an even further embodiment, the I/O means generates an audio signal. The generated characters, light emitting diode, or audio signal alert the viewer that a second unique identifier must be entered. According to yet another embodiment, the I/O means 18 does not generate a signal, but instead prevents the viewer box 2a from operating until a second unique identifier is entered.

A first unique identifier attached to the mobile agent is then compared by the control circuit 20a with the second unique identifier entered by the viewer into I/O means 18. If the unique identifiers are identical, the mobile agent is registered (i.e., stored in memory 16). Once registered, the instructions in the mobile agent are carried out by the control circuit 20a. The control circuit 20a has the ability to determine the channel of a specific selection made by the viewer and can keep track of the time spent viewing that particular channel. This information is stored in memory 16. The mobile agent will normally be operative for a specific time period. The control circuit 20a will determine when the time period has expired. Upon expiration, the control circuit will transmit the collected data back through the first I/O port 22a and connection

8 to transmitter/receiver 4. The signal carrying the collected data may be at a different frequency than the broadcast signal or mobile agent signal. Other methods for communicating two-way signals along a broadcast channel, for example, time multiplexing or the like, however, may be used. The received collected data signal is then coupled to the server control circuit 12 and the collected data signal is registered.

In order to register the collected data signal, the server control circuit 12 compares the unique identifier appended to the collected data to a plurality of unique identifiers stored in the server memory 14. If the appended unique identifier matches one of the plurality of unique identifiers stored in the server memory 14, the collected data is registered (i.e., stored in the server memory 14). The plurality of unique identifiers stored in the server memory 14 is simply a list of unique identifiers which have been assigned to individual viewers.

The means (connectors 8, 9) by which a broadcast signal and mobile agent signal are coupled to the viewer box 2 can be one-way or two-way. A one-way transmission allows data to be transmitted in only one direction (i.e., from a first location to a second location). A two-way transmission allows data to be transmitted back and forth between two locations. The first embodiment uses a two-way transmission. If the one-way transmission is selected, it is necessary to incorporate a separate path for the collected data signal to be transmitted from the viewer box 2 to the server control circuit 12.

According to a second embodiment of the invention, which is illustrated in Figure 2, and in which a one-way transmission is selected, a third I/O port 22c is connected to the server control circuit 12 through a physical connection (e.g., coaxial cable, telephone line, or fiber optic

cable). This allows the control circuit 20 to transmit the collected data signal to the server control circuit.

In the second embodiment, the control circuit 20b has a first I/O port 22a, a second I/O port 22b, and a third I/O port 22c to which electrical connections are made. The local receiver 24 receives a broadcast signal from a broadcast signal transmitter 1. The local receiver 24 is simply the means by which a broadcast signal is received at a viewer's location. The local receiver 24 can be an antenna, satellite dish, cable connection, telephone connection, fiber optic connection, or the like. The selection of the local receiver 24 depends on the method of transmission from the broadcast signal transmitter 1. The connection 9 between the broadcast signal transmitter 1 and the local receiver 24 may be a physical connection or an atmospheric connection established between, for example, satellites or antennas.

In the second embodiment, a viewer box 2b is placed in proximity to a viewer's media equipment 6. The viewer box 2b includes a control circuit 20b, an input/output ("I/O") means 18, and memory 16. The broadcast signal transmitter 1 (e.g., television transmitter, radio transmitter, and the like) transmits a broadcast signal through a transmission channel 9. The server control circuit 12 is connected to a server memory 14. The server memory 14 is a memory circuit, which is accessed and controlled by the server control circuit 12, and is a type of memory circuit known in the art. The server control circuit 12 periodically transmits a mobile agent signal to the third I/O port 22c which couples the mobile agent signal to the control circuit 20b.

Internally in the viewer box 2b, the control circuit 20b is connected to the I/O means 18 and the memory circuit 16 similar to the connections in control circuit 20a of Figure 1. The

control circuit 20b is connected to the second I/O port 22b. The second I/O port 22b is connected to media equipment 6. The control circuit 20b is also connected to the third I/O port 22c, which third I/O port 22c is connected to the server control circuit 12.

In operation, the broadcast signal transmitter 1 continuously transmits a broadcast signal to the local receiver 24. The local receiver 24 couples the broadcast signal to the first I/O port 22a. The broadcast signal is coupled by the first I/O port 22a to the control circuit 20b and is coupled from the control circuit 20b to the second I/O port 22b. The broadcast signal is then coupled by the second I/O port 22b to the media equipment 6, where it is presented to a viewer. The media equipment 6 includes televisions, radios, personal computers, and the like. The media equipment 6 is responsive to the signal coupled from the second I/O port 22b to the media equipment 6.

The server control circuit 12 transmits signals intermittently when mobile agents need to be transmitted. The mobile agent includes a set of instructions to be carried out by the control circuit 20b. The server control circuit 12 transmits a mobile agent signal to the third I/O port 22c. The third I/O port 22c then couples the mobile agent signal to the control circuit 20b. Upon receipt of a mobile agent signal, the control circuit 20b will register the signal.

The first step in registering the mobile agent is to request that the viewer enter a second unique identifier into the I/O means 18. The control circuit 20b instructs I/O means 18 to request entry of the second unique identifier by the viewer. According to one embodiment, the I/O means 18 generates characters, which are coupled through the control circuit 20b to the media equipment 6 and displayed. According to another embodiment, the I/O means 18 illuminates a light emitting diode. According to an even further embodiment, the I/O means 18 generates an

audio signal. The generated characters, light emitting diode, or audio signal alert the viewer that the second unique identifier must be entered. According to a still further embodiment, the I/O means 18 prevents the viewer box 2b from operating until a second unique identifier is entered. Once registered, the mobile agent is stored in the memory 16 and the instructions in the mobile agent are carried out by the control circuit 20b.

The control circuit 20b has the ability to determine the channel of a specific selection made by the viewer and can keep track of the time spent viewing that particular selection. This information is stored in memory 16. The mobile agent will normally be operative for a specific time period. The control circuit will determine when the time period has expired. Upon expiration, the control circuit will transmit the collected data back through the third I/O port 22c to the server control circuit 12. The collected data signal is registered by the server control circuit 12. Once registered, the collected data is stored in the server memory 14.

In an alternative embodiment, a physical connection between the I/O port 22c and the server control circuit 12 is not necessary. The data can be transmitted via a cellular telephone system or other low power atmospheric transmission system known in the art. The low power atmospheric transmission system would include a low power atmospheric transmitter/receiver, a low power atmospheric transmitter/receiver controller, a two-way low power atmospheric transmitter/receiver port, and a one-way or two-way communication port connected between the control circuit and media equipment. The low power atmospheric transmitter/receiver is any transmitter or receiver known in the art, for example, transmitters and receivers currently used in cellular systems, personal communication services ("PCS"), and two-way radio systems. The low power atmospheric transmitter/receiver controller is a logic circuit known in the art to control a transmitter or receiver. In this alternative embodiment, a two-way transmission means

is established without having to make a physical connection between the server control circuit 12 and the viewer box 2b.

Referring to Figure 3, the steps of a method for viewer identification and data collection verification according to an embodiment of the invention will be described in detail. The first step is to assign a first unique identifier to a viewer 100. This may be done at secure sites (e.g., branch offices, secure internet access), which will verify a viewer's identity and assign a first unique identifier to that identity. The first unique identifier can be an alphanumeric sequence chosen from a list of alphanumeric sequences (hereinafter referred to as a personal identification number or "PIN"). Alternatively, the first unique identifier is a digitized representation of a body characteristic (e.g., thumbprint). According to one embodiment, the step of assigning a first unique identifier includes submitting a unique biological identifier (e.g., fingerprint, retinal scan) which is converted into a digital code.

According to one embodiment, a digitized body characteristic may be formed from, for example, a digitized image of the viewer's fingerprint, iris, or retina. Other physical characteristics may be used, depending on the degree of security desired, for example, an image of the registrant's footprint, handprint, dental x-ray, or other distinguishing characteristic of the registrant's body. Through an encryption process, an example of which is detailed in co-pending United States Patent Application Serial Number 09/123,793 titled "Non-reputable Digital Signature Based on Biological Indicia," and which is herein incorporated by reference, a digital certificate is formed and the first unique identifier includes the digital certificate.

The first unique identifier and viewer's identity are then stored 102 in memory 14, which is accessible to the server control circuit 12. When the first unique identifier is stored 102, it is

cross-referenced to the viewer's identity so that either the first unique identifier or the viewer's identity can be accessed by having the other. The server control circuit 12 then generates 104 a public/private key pair, which can be generated using a means known in the art, such as RSA, PGP, El Gamal public key encryption techniques, and the like. The public key is an encryption key and the private key is a decryption key. One key cannot be derived from the other. The first unique identifier is then encrypted 106 using the public key. The result is an encrypted unique identifier. The public key and private key are then stored 108 in memory 14 and cross-referenced to the first unique identifier and viewer identity data. A mobile agent is then generated 109 by the server circuit and the private key and public key are appended 110 to the mobile agent which results in a keyed mobile agent. The keyed mobile agent is then encrypted 112 using the first unique identifier. The result is an encrypted keyed mobile agent. The encrypted unique identifier is then appended to the encrypted keyed mobile agent 114 forming a unique encrypted keyed mobile agent. The unique encrypted keyed mobile agent is then transferred 116 to a second location.

According to one embodiment of the invention, the second location is a viewer box 2a, 2b that is attached to media equipment 6. Upon receiving 118 the unique encrypted keyed mobile agent, the viewer box 2a, 2b will request 120 that the viewer enter a second unique identifier that had been assigned earlier. The unique identifier, which is entered in response to the request from the viewer box, will be referred to as the second unique identifier and may be identical to the first unique identifier. The viewer enters 122 the second unique identifier through any input means known in the art. Entry can be accomplished by several methods including punching in an alphanumeric sequence on a keypad or by inserting an appendage in a print reader. Once the second unique identifier has been received 124, a control circuit 20a, 20b in the viewer box 2a, 2b separates 126 the unique encrypted keyed mobile agent into an

encrypted unique identifier and an encrypted keyed mobile agent. The second unique identifier is then used to decrypt 128 the encrypted keyed mobile agent to generate a data string. If the second unique identifier is identical to the first unique identifier, the data string will be the keyed mobile agent. The keyed mobile agent is then separated 130 into the private key, public key, and mobile agent. If the second unique identifier is not identical to the first unique identifier, the data string will not be the keyed mobile agent and may be unintelligible data. Using the private key, the encrypted unique identifier is decrypted 132. The second unique identifier is then compared 134 to the first unique identifier.

According to one embodiment of the invention, the system includes a plurality of viewer boxes 2a, 2b, which are remotely located. Each mobile agent is created specifically for an individual viewer. The server circuit 12 transmits identical copies of the individualized mobile agent to each of the plurality of viewer boxes 2a, 2b. If the second unique identifier and first unique identifier are different, the mobile agent has been received by the wrong viewer box 2a, 2b and an error message is returned 136 to the server control circuit 12. If the identifiers are identical, then the mobile agent has been received by the correct viewer box 2a, 2b and the mobile agent is stored 138 in memory in the viewer box 2a, 2b. The mobile agent, private key, and public key are stored 138 in the viewer box memory 16.

The only way that the first unique identifier and the second unique identifier can be identical is if the private key is decrypted with the exact same key with which it was encrypted (i.e., the first unique identifier) and the first unique identifier is decrypted with the private key which correctly corresponds to the public key which encrypted the first unique identifier. If both the encrypted private key and encrypted first unique identifier are not properly decrypted, the first unique identifier and second unique identifier will not be identical.

The viewer box receives a plurality of broadcast signals 140. Once the mobile agent has been stored in memory 16, the instruction set is carried out. The mobile agent's instruction set instructs the viewer box 2a, 2b to begin collecting 142 and storing 144 data regarding the viewer's selection of broadcast signals. According to one embodiment, the mobile agent will include a time of expiration. The viewer box 2a, 2b keeps track of the time and checks to make sure the time has not expired 146. As long as time has not expired, the viewer box 2a, 2b collects 142 and stores 144 data. If time has expired, however, the mobile agent issues commands to the viewer box 2a, 2b to cease collecting data and to replicate the mobile agent. The collected data is then appended 148 to the replica of the mobile agent forming a data agent. The data agent is then encrypted 150 using the public key forming an encrypted data agent. The unique identifier is then appended 152 to the encrypted data agent forming a unique encrypted data agent. It is not necessary to specify that the first or second unique identifier is appended 152, because this step cannot be reached unless the first and second unique identifiers are identical.

The unique encrypted data agent is then transferred 154 to a first location. According to one embodiment, the first location is the server control circuit 12. Upon receipt 156 of the unique encrypted data agent at the server control circuit 12, the unique encrypted data agent is separated 158 into the unique identifier and the encrypted data agent. The server control circuit 12 compares 160 the unique identifier to a list of unique identifiers contained in memory. If none of the unique identifiers in memory match the unique identifier, an error message is triggered 162. If there is a match, the server control circuit 12 cross-references 164 the matched unique identifier in memory and retrieves 166 the associated private key. The private key is then used to decrypt 168 the encrypted data agent. The server control circuit 12 then separates 170

the collected data and mobile agent and the collected data is stored 172 in the server control circuit memory 14. The method ensures that only the viewer having a specific unique identifier may add data to the stored collected data by positively identifying the viewer. Market analysts, therefore, may rely on the data in planning market strategies.

An alternative embodiment of the present invention is illustrated in the flowchart of Figure 4. Similar to the method detailed with respect to Figure 3, a first unique identifier is assigned 174 to a recipient. The first unique identifier is stored 176 in memory 14 and cross-referenced to the identity of the recipient. A public/private key pair is then generated 178 and the first unique identifier is encrypted 180 using the public key. The public key and private key are then stored 182 in memory 14 with cross-references to the recipient's identity. The private key and public key are then encrypted 184 using the first unique identifier forming encrypted keys. The encrypted keys are appended 186 to the encrypted unique identifier forming unique encrypted keys. The unique encrypted keys are transmitted 188 to a second location. Upon receipt 190 of the unique encrypted keys at the second location, a request is made 192 for the recipient to enter the second unique identifier that had been assigned earlier. The recipient enters 194 the second unique identifier and the second unique identifier is received 196 by a control circuit 20a, 20b. The unique encrypted keys are then separated 198 into the encrypted unique identifier and the encrypted keys. The second unique identifier is then used to decrypt 200 the encrypted keys. The private key is then used to decrypt 202 the encrypted unique identifier. The second unique identifier is then compared 204 to the first unique identifier. If they are different, an error message is generated and transmitted 208 to the first location. If they are identical, the decrypted keys are stored 206 in memory at the second location. This alternative method provides only one-way transfer from a first location to a second location. The advantage of this method is that the public key and private key can be securely transferred to a remote location

because the keys can only be properly decrypted and stored in memory if the viewer enters the correct unique identifier. The public key can then be used to encrypt data which is to be transmitted back to the first location.

Referring to Figure 5, another embodiment of the present invention will be described in detail. Figure 5 is a flowchart illustrating a method of viewer identification and data collection verification which does not use encryption technology. The viewer is assigned 210 a first unique identifier and the first unique identifier is stored 212 in memory 14 along with a cross-reference to the viewer's identity. A mobile agent is then generated 213 and the first unique identifier is appended 214 to the mobile agent forming a unique mobile agent. The unique mobile agent is then transferred 216 to a second location, for example a viewer box 2a, 2b, and is registered 218. The unique mobile agent is registered 218 by requesting the viewer enter a second unique identifier that was previously assigned and comparing the second unique identifier to the first unique identifier appended to the mobile agent. If they are different, an error message is generated. If they are identical, the mobile agent is stored in memory. A plurality of broadcast signals are received 220 at the second location and the viewer selects 222 one of the plurality to view. The selection 222 is recorded 224 until a timer expires. After the timer expires, the unique identifier is appended 226 to the collected data forming unique data. The unique data is then transferred 228 to the first location, for example, a server control circuit 12, and is registered 230. The unique data is registered 230 by comparing the unique identifier with unique identifiers stored in memory 14 at the first location. If they do not match, an error message is generated. If they do match, the collected data is stored 232 in memory at the first location.

Although the illustrative embodiments of the present invention have been described herein with reference to the accompanying drawings, it is to be understood that the invention is

not limited to those precise embodiments, and that various other changes and modifications may be effected therein by one skilled in the art without departing from the scope or spirit of the invention.

TABLE OF DEFINITIONS

Broadcast Signal—Transmitted information, such as televisions signals, radio signals, and the like.

Collected Data—The information which is collected by the viewer box and which includes the designation for the selected broadcast signal and the time elapsed while viewing the selected broadcast signal.

Combined Signal—A single signal that includes both the mobile agent and broadcast signal.

Data String—The decrypted first unique identifier.

Decrypted Data Agent—The encrypted data agent after it has been decrypted using the private key.

Decrypted Keyed Mobile Agent—The encrypted keyed mobile agent after it is separated from the unique encrypted keyed mobile agent and decrypted using the second unique identifier.

Encrypted Data Agent—The encrypted mobile agent with the collected data appended to it.

Encrypted Keyed Mobile Agent—The keyed mobile agent which has been encrypted using the first unique identifier.

Encrypted Unique Identifier—The first unique identifier which has been encrypted using the public key.

First Unique Identifier—The digital code assigned to a viewer.

Keyed Mobile Agent—The mobile agent with the public/private key pair appended to it.

Mobile Agent—A digital code which can include a set of commands to be executed by a processor and can also include biographic or demographic information of a viewer.

Second Unique Identifier—The digital code entered into a viewer box by a viewer to verify the viewer's identity.

Unique Encrypted Data Agent--The second unique identifier which has been appended to the encrypted data agent.

Unique Encrypted Keyed Mobile Agent—The encrypted keyed mobile agent with the encrypted unique identifier appended to it.

Unique Identifier—A digital code assigned to a specific person, which digital code can be a personal identification number or digitized biological indicia.

We claim:

1. A method of identifying a viewer comprising the steps of:

assigning a first unique identifier to a viewer;

storing the first unique identifier at a first location;

encrypting the first unique identifier to form an encrypted unique identifier;

generating a mobile agent;

encrypting the mobile agent to form an encrypted mobile agent;

appending the encrypted unique identifier to the encrypted mobile agent to form a unique encrypted mobile agent;

transferring the unique encrypted mobile agent from the first location to a second location;

receiving a second unique identifier from the viewer at the second location;

separating the encrypted mobile agent from the encrypted unique identifier;

decrypting the encrypted mobile agent using the second unique identifier;

decrypting the encrypted unique identifier to form a data string;

comparing the data string to the second unique identifier; and

storing the mobile agent in memory at the second location if the data string and the second unique identifier are identical.

2. The method as defined by claim 1, wherein the step of assigning a first unique identifier comprises:

selecting a unique alphanumeric sequence;

assigning the unique alphanumeric sequence to the viewer; and

storing the assignment of the unique alphanumeric sequence to the viewer in a memory at the first location.

3. The method according to claim 2, wherein the step of assigning further comprises storing a list of unused alphanumeric sequences in the memory and removing the selected unique alphanumeric sequence from the list.

4. The method as defined by claim 1, wherein the step of assigning a first unique identifier comprises:

creating a digital representation of a body characteristic of the viewer;

assigning the digital representation to the viewer; and

recording the assignment of the digital representation to the viewer in memory at the first location.

5. The method as defined by claim 4, wherein the step of creating a digital representation of a body characteristic of a viewer comprises:

placing an eye of the viewer in proximity to a retinal scanner;

scanning a retina of the eye by the retinal scanner; and

creating a digital representation of the retina.

6. The method of viewer identification as defined by claim 4, wherein the step of creating a digital representation of a body characteristic of a viewer comprises:

inserting an appendage of the viewer into a print reader;

scanning the appendage by the print reader; and

creating a digital representation of the appendage.

7. The method as defined by claim 6, wherein the appendage is a digit of the viewer's hand.

8. The method as defined by claim 1, wherein the steps of encrypting use one or more keys.

9. The method as defined by claim 1, wherein the step of encrypting the mobile agent comprises:

creating a digital word including the mobile agent;

appending a key to the digital word in a data stream;

appending a marker to the data stream, the marker indicating starting positions of the key and mobile agent in the data stream; and

encrypting the data stream.

10. The method as defined by claim 1, wherein the step of separating comprises:

locating a marker in the transferred unique encrypted mobile agent, the marker indicating starting points for the encrypted mobile agent and the encrypted unique identifier; and

separating the unique encrypted mobile agent into the encrypted mobile agent and the encrypted unique identifier using the marker.

11. The method as defined by claim 1, wherein the step of appending the encrypted unique identifier to the encrypted mobile agent comprises:

creating a digital word including the encrypted mobile agent;

appending the encrypted unique identifier to the digital word; and

appending a marker to the digital word, the marker indicating starting positions of the encrypted mobile agent and encrypted unique identifier in the digital word.

12. The method as defined by claim 1, further comprising requesting a second unique identifier from the viewer at the second location.

13. The method as defined by claim 12, wherein the step of requesting a second unique identifier from the viewer comprises:

determining that the unique encrypted keyed mobile agent has been received at the second location; and

outputting a message to the viewer to enter the second unique identifier.

14. The method as defined by claim 13, wherein the step of outputting the message to the viewer to enter the second unique identifier comprises displaying the message on an alphanumeric display.

15. The method as defined by claim 13, wherein the step of outputting the message to the viewer to enter the second unique identifier comprises illuminating an indicator light.

16. The method as defined by claim 13, wherein the step of outputting the message to the viewer to enter the second unique identifier comprises generating an audio signal.

17. The method as defined by claim 1, wherein the step of receiving the second unique identifier comprises entering a personal identification number on a keypad.

18. The method as defined by claim 1, wherein the step of receiving the second unique identifier comprises:

digitizing a unique biological identifier; and

receiving the digitized unique biological identifier.

19. The method as defined by claim 18, wherein the step of digitizing the unique biological identifier comprises:

placing an eye of the viewer in proximity to a retinal scanner;

scanning a retina of the eye by the retinal scanner; and

creating a digital representation of the retina.

20. The method as defined by claim 18, wherein the step of digitizing the unique biological identifier comprises:

inserting an appendage of the viewer into a print reader;

scanning the appendage by the print reader; and

creating a digital representation of the appendage.

21. The method as defined by claim 20, wherein the appendage is a digit of the viewer's hand.

22. The method as defined by claim 1, wherein the step of separating comprises:

locating a marker in the transferred encrypted mobile agent and the encrypted unique identifier; and

separating the encrypted mobile agent and the encrypted unique identifier using the marker.

23. The method as defined by claim 1, wherein the steps of decrypting uses one or more keys.

24. The method as defined by claim 1, further comprising the step of generating a public key/private key pair at the first location.

25. The method as defined by claim 24, wherein the step of encrypting the mobile agent comprises:

appending the public key to the mobile agent;

appending the private key to the public key and mobile agent; and

encrypting the public key, private key, and mobile agent.

26. The method as defined by claim 25, wherein the step of appending the public key to the mobile agent comprises:

creating a digital word including the mobile agent;

appending the public key to the digital word; and

appending a marker to the digital word, the marker indicating starting positions of the public key and mobile agent.

27. The method as defined by claim 25, wherein the step of appending the private key comprises:

forming a digital word including the private key, the public key, and the mobile agent; and

appending a marker to the digital word, the marker indicating starting positions of the private key, public key, and mobile agent.

28. The method as defined by claim 24, wherein the step of decrypting the encrypted mobile agent using the second unique identifier further comprises the step of separating the public key, private key, and mobile agent.

29. The method as defined by claim 24, further comprising the step of storing the public key in a memory at the first location.

30. The method as defined by claim 24, further comprising the step of storing the private key in a memory at the first location.

31. The method as defined by claim 24, wherein the private key is used to decrypt the encrypted unique identifier.

32. The method as defined by claim 24, wherein the public key is used to encrypt the first unique identifier.

33. A method of identifying a viewer comprising the steps of:

assigning a first unique identifier to the viewer;

storing the first unique identifier in a memory at a first location;

appending the first unique identifier to a mobile agent to form a unique mobile agent, the mobile agent including a set of commands;

transmitting the unique mobile agent to a second location; and

registering the unique mobile agent at the second location.

34. The method as defined in claim 33, wherein the step of registering the unique mobile agent comprises the steps of:

receiving a second unique identifier from the viewer at the second location;

comparing the second unique identifier to the first unique identifier appended to the mobile agent; and

storing the mobile agent at the second location if the second unique identifier and the first unique identifier match.

35. A method of viewer identification comprising:

generating a unique digital code;

transferring the unique digital code to a plurality of remote locations;

receiving a plurality of identifiers from a corresponding plurality of viewers at the plurality of remote locations;

comparing the plurality of identifiers to the unique digital code to find a match; and

storing the unique digital code at a remote location where there is a match.

36. The method of viewer identification as defined by claim 35, further comprising the step of generating an error signal at remote locations where there is no match.

37. The method of viewer identification as defined by claim 35, wherein the step of transferring the unique digital code to the plurality of remote locations comprises transferring the unique digital code to the plurality of remote locations at substantially the same time.

38. A method for verification of collected data comprising the steps of:

receiving a plurality of broadcast signals at a viewer location;

collecting data at the viewer location;

appending the collected data to a mobile agent at the viewer location to form a data agent;

encrypting the data agent to form an encrypted data agent;

appending a first unique identifier to the encrypted data agent to form a unique encrypted data agent;

transferring the unique encrypted data agent to a central location;

separating the first unique identifier from the unique encrypted data agent;

identifying a viewer associated with the first unique identifier;

decrypting the encrypted data agent;

separating the collected data from the data agent; and

associating the collected data with the viewer.

39. The method for verification of collected data as defined by claim 38, wherein the broadcast signals comprise at least one of a plurality of television, radio, and computer network programs.

40. The method for verification of collected data as defined by claim 38, further comprising comparing the first unique identifier to at least one of a plurality of unique identifiers stored at the central location and determining whether the first unique identifier matches one of the plurality of unique identifiers stored at the central location.

41. The method for verification of collected data as defined by claim 38, wherein the step of encrypting the data agent to form an encrypted data agent uses an encryption key.

42. The method for verification of collected data as defined by claim 41, wherein the encryption key is a public key, the public key being part of a public key/private key pair.

43. The method for verification of collected data as defined by claim 41, wherein the step of identifying a viewer further comprises retrieving an encryption key associated with the identified viewer.

44. The method for verification of collected data as defined by claim 43, wherein the encryption key is a public key, the public key being part of a public key/private key pair.

45. The method for verification of collected data as defined by claim 41, wherein the step of decrypting the encrypted data agent uses a key.

46. The method for verification of collected data as defined by claim 45, wherein the key is a private key, the private key being part of a public key/private key pair.

47. The method of verification of collected data as defined by claim 38, wherein the step of appending the collected data to a mobile agent comprises:

creating a digital word including the mobile agent;

appending the collected data to the digital word; and

appending a marker to the digital word, the marker indicating starting positions of the collected data and mobile agent.

48. The method of verification of collected data as defined by claim 47, wherein the step of separating the collected data from the data agent comprises:

extracting the marker from the digital word; and

separating the collected data and the mobile agent into individual digital words using starting positions indicated by the marker.

49. The method of verification of collected data as defined by claim 38, wherein the step of appending the first unique identifier to the encrypted data agent comprises:

creating a digital word including the encrypted data agent;

appending the first unique identifier to the digital word; and

appending a marker to the digital word, the marker indicating starting positions of the first unique identifier and encrypted data agent.

50. The method of verification of collected data as defined by claim 49, wherein the step of separating the first unique identifier from the unique encrypted data agent comprises:

extracting the marker from the digital word; and

separating the first unique identifier from the unique encrypted data agent based on starting positions indicated by the marker.

51. The method of verification of collected data as defined by claim 38, wherein the step of collecting data at the second location comprises:

determining a broadcast channel selected by the viewer from the plurality of channels;

recording the selected broadcast channel in a memory at the viewer location; and

recording the elapsed time viewing the selected broadcast channel in the memory.

52. A viewer box for a system for viewer identification and verification of collected data connected to media equipment, the viewer box comprising:

control means for outputting a message when a mobile agent signal is received;

receiving means coupled to the control means and the media for receiving a plurality of broadcast signals from a remote location and for displaying a selected signal on the media equipment;

means for inputting data to the control means by the viewer;

means for identifying the broadcast signal responsive to the control means;

data collection means for collecting data regarding the selected signal;

means for transmitting the collected data.

53. A viewer box for a system for identification of a viewer and verification of collected data connected to media equipment, the viewer box comprising:

a control circuit adapted to detect which of a plurality of channels is selected and the time spent viewing the selected channel;

a memory circuit electrically connected to the control circuit, the memory circuit adapted to store data regarding the selected channel and time;

an input means electrically connected to the control circuit adapted to receive a unique identifier from the viewer; and

an output means electrically connected to the control circuit adapted to prompt a viewer to enter the unique identifier.

54. The viewer box as defined by claim 53, wherein the control circuit further comprises:

a two-way communication port connected between the control circuit and a transmitter/receiver; and

one of a one-way and a two-way communication port connected between the control circuit and a media equipment.

55. The viewer box as defined by claim 53, wherein the input means comprises a retinal scanner.

56. The viewer box as defined by claim 53, wherein the input means comprises a reader adapted to read a fingerprint.

57. The viewer box as defined by claim 53, wherein the input means comprises an alphanumeric keypad.

58. The viewer box as defined by claim 53, wherein the unique identifier is a personal identification number.

59. The viewer box as defined by claim 53, wherein the data unique identifier is a digital representation of a body characteristic.

60. The viewer box as defined by claim 53, wherein the control circuit further comprises:

at least one of a one-way and a two-way communication port connected between the control circuit and a transmitter/receiver;

at least one of a one-way and a two-way communication port connected between the control circuit and a media equipment; and

a two-way communication port connected between the control circuit and a server circuit.

61. The viewer box as defined by claim 53, wherein the control circuit further comprises:

a low power atmospheric transmitter/receiver connected to the control circuit;

a low power atmospheric transmitter/receiver controller adapted to control the low power atmospheric transmitter/receiver;

a two-way low power atmospheric transmitter/receiver port connected to the control circuit; and

at least one of a one-way and a two-way communication port connected between the control circuit and media equipment.

62. The viewer box as defined by claim 53, further comprising an alphanumeric keypad having a plurality of keys, at least one key being adapted to read a fingerprint when at least one key is depressed.

63. A system for viewer identification and verification of collected data comprising:

a transmitter adapted to transmit a combined signal including a broadcast signal and a mobile agent signal;

a viewer box, the viewer box being connected to the transmitter by at least one communication channel;

a server circuit, the server circuit including a server control circuit and a server memory, the server control circuit electrically connected to the transmitter and the server memory;

a receiver connected with the viewer box by at least one communication channel and electrically connected with the server circuit, the receiver receiving a data signal transmitted from the viewer box across the at least one communication channel; and

media equipment, the media equipment connected with the viewer box and adapted to display the broadcast signal.

64. The system for viewer identification and verification of collected data as defined by claim 63, wherein the viewer box further comprises an alphanumeric keypad.

65. The system for viewer identification and verification of collected data as defined by claim 63, wherein the viewer box further comprises a reader adapted to read a fingerprint.

66. The system for viewer identification and verification of collected data as defined by claim 63, wherein the viewer box further comprises retinal scanner.

67. A system for viewer identification comprising:

means for transmitting a broadcast signal;

means for transmitting a mobile agent signal, the mobile agent signal including a set of commands;

means for receiving the broadcast signal and mobile agent signal, the means for receiving being responsive to the means for transmitting a broadcast signal and the means for transmitting a mobile agent signal;

display means for displaying the broadcast signal to the viewer, the display means being responsive to the broadcast signal and the means for receiving coupling the broadcast signal to a display means;

control means for receiving a mobile agent and viewer identifying information and for keeping track of time;

means for inputting data to the control means by a viewer and verifying means for comparing the viewer identifying information with second viewer identifying information of the viewer.

68. A system for verification of collected data comprising:

receiving means for receiving a plurality of broadcast signals and a mobile agent signal;

means for collecting data;

control means for encrypting the mobile agent and the collected data;

memory means for storing the collected data connected with the control means;

transmitting means for transmitting collected data, the mobile agent, and one or more encryption keys to a remote location and connected with the control means;

means for receiving the collected data transmitted by the transmitting means and for identifying a viewer associated with the collected data; and

means for storing the collected data after the viewer has been identified.

69. A method for securely transferring a public key/private key pair from a first location to a second location for use in system to identify a viewer and to verify collected data, comprising the steps of:

assigning a first unique identifier to the viewer;

generating a public/private key pair;

encrypting the first unique identifier using the public key to form an encrypted unique identifier;

encrypting the public key and private key using the first unique identifier to form encrypted keys;

appending the encrypted unique identifier to the encrypted keys to form unique encrypted keys;

transferring the unique encrypted keys from the first location to the second location;

entering a second unique identifier of the viewer;

separating the encrypted keys from the encrypted unique identifier;

decrypting the encrypted keys using the second unique identifier to form decrypted keys;

decrypting the encrypted unique identifier using the private key to form a data string;

comparing the data string to the second unique identifier; and

storing the decrypted keys at the second location if the data string and the second unique identifier match.

70. The method as defined by claim 69, wherein the step of assigning a first unique identifier comprises:

selecting a unique alphanumeric sequence of a predetermined length from a list of unused alphanumeric sequences;

assigning the unique alphanumeric sequence to the viewer;

recording the assignment of the unique alphanumeric sequence to the viewer in a memory at the first location; and

removing the unique alphanumeric sequence from the list of unused alphanumeric sequences in the memory.

71. The method as defined by claim 69, wherein the step of assigning the first unique identifier comprises:

creating a digital representation of a body characteristic of the viewer;

assigning the digital representation to the viewer; and

recording the assignment of the digital representation to the viewer in the memory at the first location.

72. The method as defined by claim 71, wherein the step of creating the digital representation of the body characteristic of the viewer comprises:

placing an eye of the viewer in proximity to a retinal scanner;

scanning a retina of the eye by the retinal scanner; and

creating a digital representation of the retina.

73. The method as defined by claim 71, wherein the step of creating the digital representation of the body characteristic of the viewer comprises:

inserting an appendage of the viewer into a print reader;

scanning the appendage by the print reader; and

creating a digital representation of the appendage's print.

74. The method as defined by claim 73, wherein the appendage is a digit of the viewer's hand.

75. The method as defined by claim 69, wherein the step of appending the encrypted unique identifier to the encrypted keys comprises:

creating a digital word including the encrypted keys;

appending the encrypted unique identifier to the digital word; and

appending a marker to the digital word, the marker indicating starting positions of the encrypted keys and encrypted unique identifier.

76. The method as defined by claim 69, wherein the step of separating the encrypted keys from the encrypted unique identifier comprises:

extracting a marker from a data stream, the data stream including the encrypted mobile agent and the encrypted unique identifier, the marker indicating starting points in the data stream for the encrypted mobile agent and encrypted unique identifier; and

separating the encrypted mobile agent and encrypted unique identifier into individual digital words using the starting points indicated by the marker.

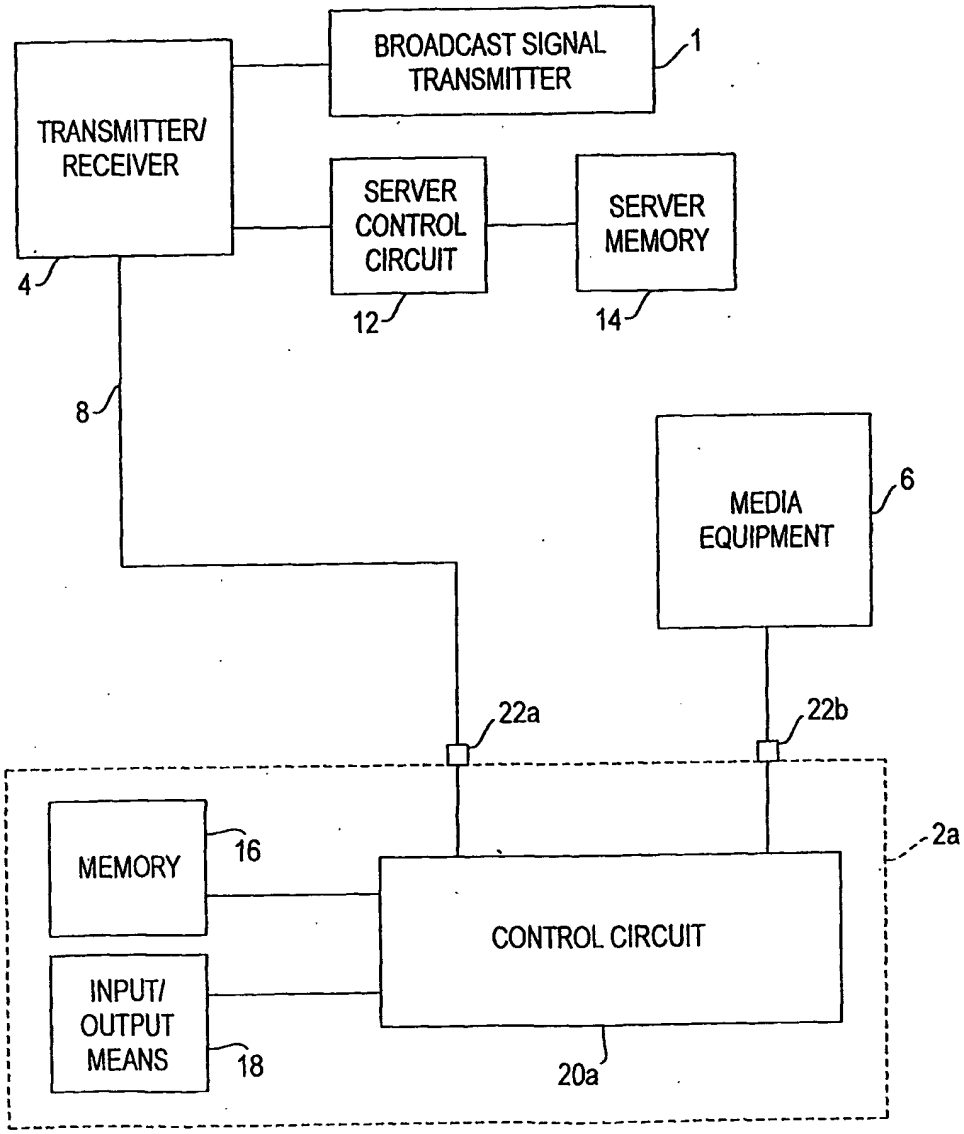

BROADCAST SIGNAL TRANSMITTER
1
TRANSMITTER/ RECEIVER
4
SERVER CONTROL CIRCUIT
12
SERVER MEMORY
14
8
MEDIA EQUIPMENT
6
22a
22b
2a
MEMORY
16
CONTROL CIRCUIT
INPUT/ OUTPUT MEANS
18
20a

FIG. 1

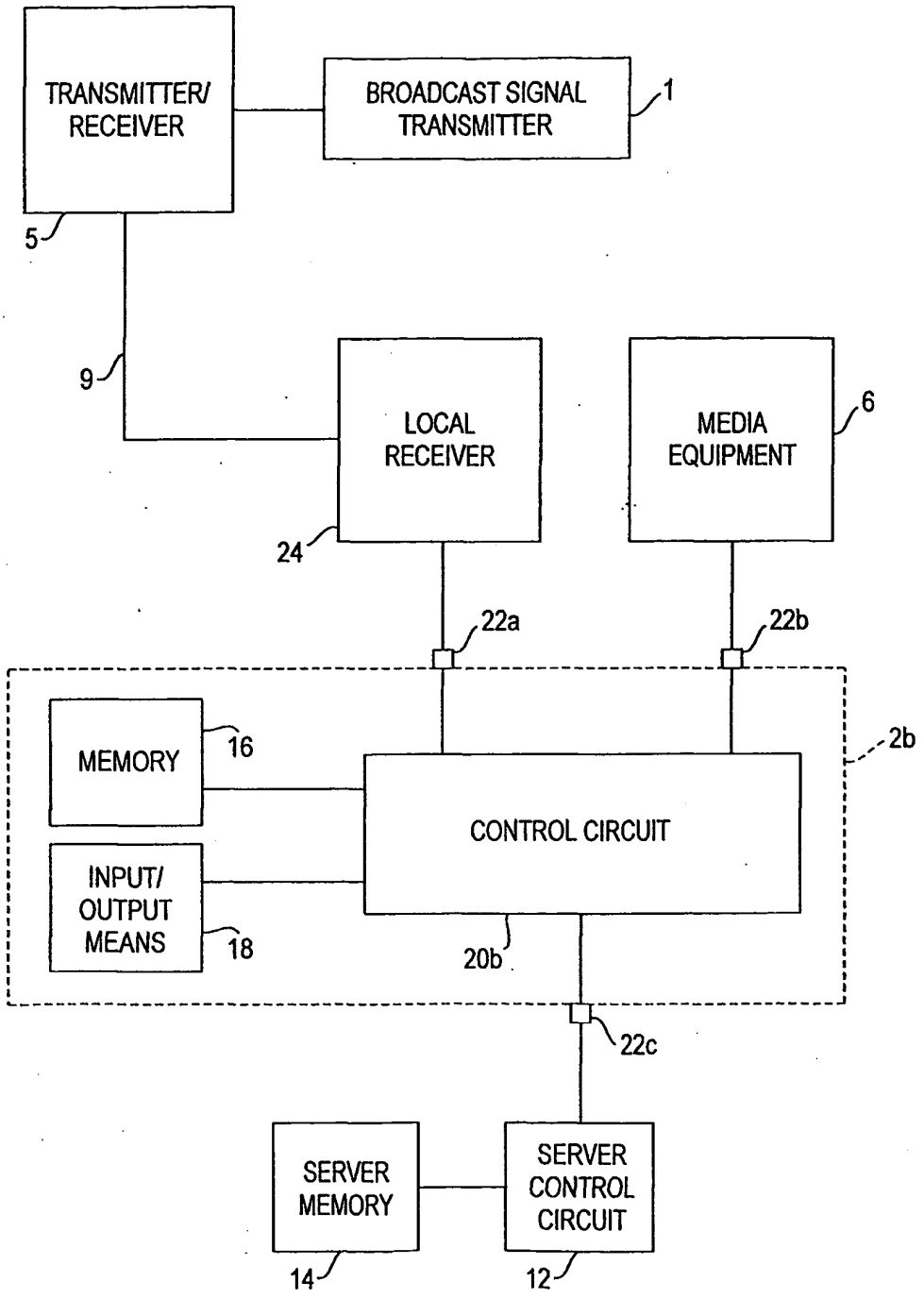

TRANSMITTER/ RECEIVER
BROADCAST SIGNAL TRANSMITTER
1
5
9
LOCAL RECEIVER
MEDIA EQUIPMENT
6
24
22a
22b
MEMORY
16
CONTROL CIRCUIT
2b
INPUT/ OUTPUT MEANS
18
20b
22c
SERVER MEMORY
SERVER CONTROL CIRCUIT
14
12

FIG. 2

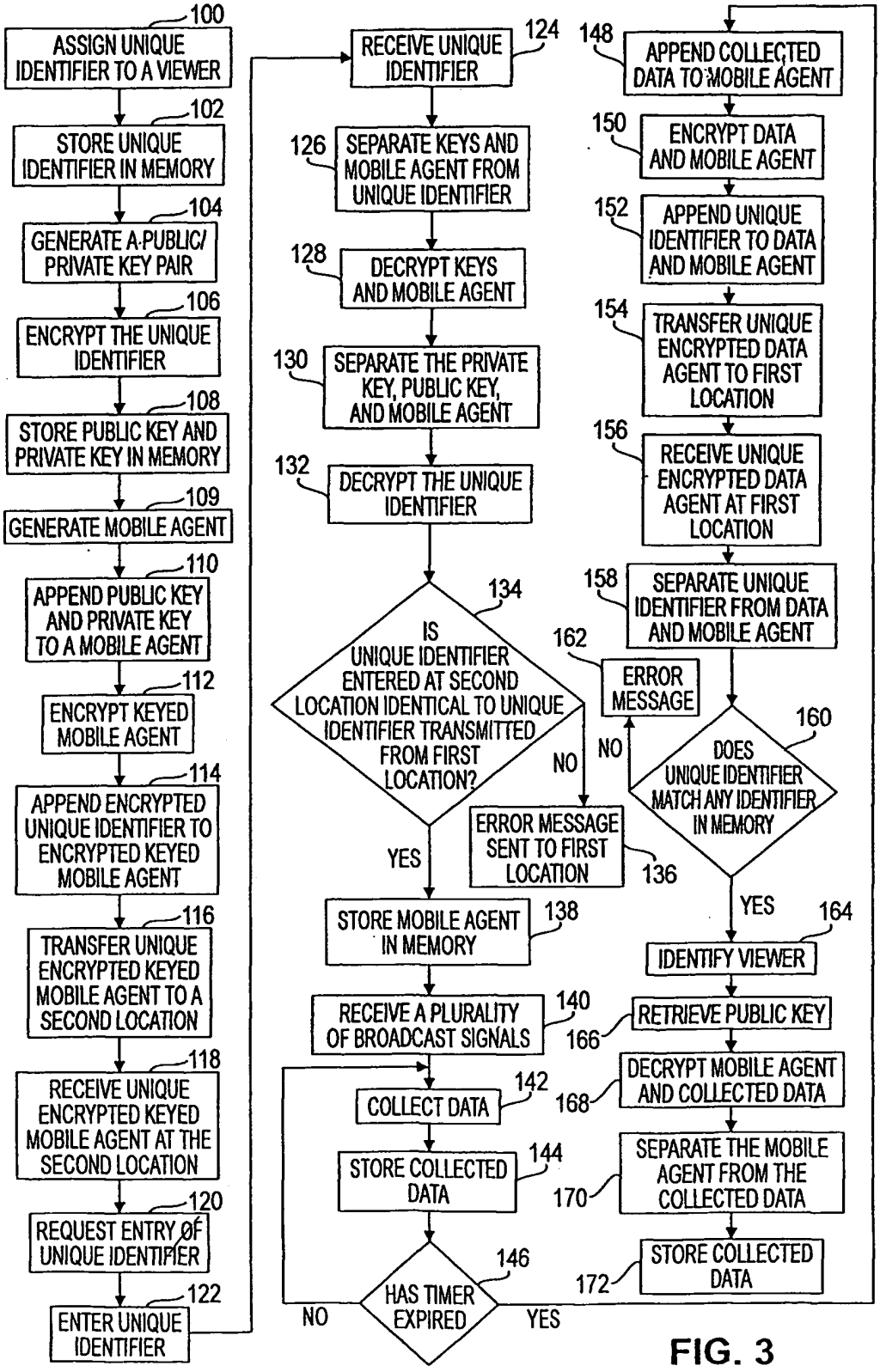

100
ASSIGN UNIQUE IDENTIFIER TO A VIEWER
102
STORE UNIQUE IDENTIFIER IN MEMORY
104
GENERATE A PUBLIC/ PRIVATE KEY PAIR
106
ENCRYPT THE UNIQUE IDENTIFIER
108
STORE PUBLIC KEY AND PRIVATE KEY IN MEMORY
109
GENERATE MOBILE AGENT
110
APPEND PUBLIC KEY AND PRIVATE KEY TO A MOBILE AGENT
112
ENCRYPT KEYED MOBILE AGENT
114
APPEND ENCRYPTED UNIQUE IDENTIFIER TO ENCRYPTED KEYED MOBILE AGENT
116
TRANSFER UNIQUE ENCRYPTED KEYED MOBILE AGENT TO A SECOND LOCATION
118
RECEIVE UNIQUE ENCRYPTED KEYED MOBILE AGENT AT THE SECOND LOCATION
120
REQUEST ENTRY OF UNIQUE IDENTIFIER
122
ENTER UNIQUE IDENTIFIER
124
RECEIVE UNIQUE IDENTIFIER
126
SEPARATE KEYS AND MOBILE AGENT FROM UNIQUE IDENTIFIER
128
DECRYPT KEYS AND MOBILE AGENT
130
SEPARATE THE PRIVATE KEY, PUBLIC KEY, AND MOBILE AGENT
132
DECRYPT THE UNIQUE IDENTIFIER
134
IS UNIQUE IDENTIFIER ENTERED AT SECOND LOCATION IDENTICAL TO UNIQUE IDENTIFIER TRANSMITTED FROM FIRST LOCATION?
NO
YES
136
ERROR MESSAGE SENT TO FIRST LOCATION
138
STORE MOBILE AGENT IN MEMORY
140
RECEIVE A PLURALITY OF BROADCAST SIGNALS
142
COLLECT DATA
144
STORE COLLECTED DATA
146
HAS TIMER EXPIRED
NO
YES
148
APPEND COLLECTED DATA TO MOBILE AGENT
150
ENCRYPT DATA AND MOBILE AGENT
152
APPEND UNIQUE IDENTIFIER TO DATA AND MOBILE AGENT
154
TRANSFER UNIQUE ENCRYPTED DATA AGENT TO FIRST LOCATION
156
RECEIVE UNIQUE ENCRYPTED DATA AGENT AT FIRST LOCATION
158
SEPARATE UNIQUE IDENTIFIER FROM DATA AND MOBILE AGENT
160
DOES UNIQUE IDENTIFIER MATCH ANY IDENTIFIER IN MEMORY
NO
162
ERROR MESSAGE
YES
164
IDENTIFY VIEWER
166
RETRIEVE PUBLIC KEY
168
DECRYPT MOBILE AGENT AND COLLECTED DATA
170
SEPARATE THE MOBILE AGENT FROM THE COLLECTED DATA
172
STORE COLLECTED DATA

FIG. 3

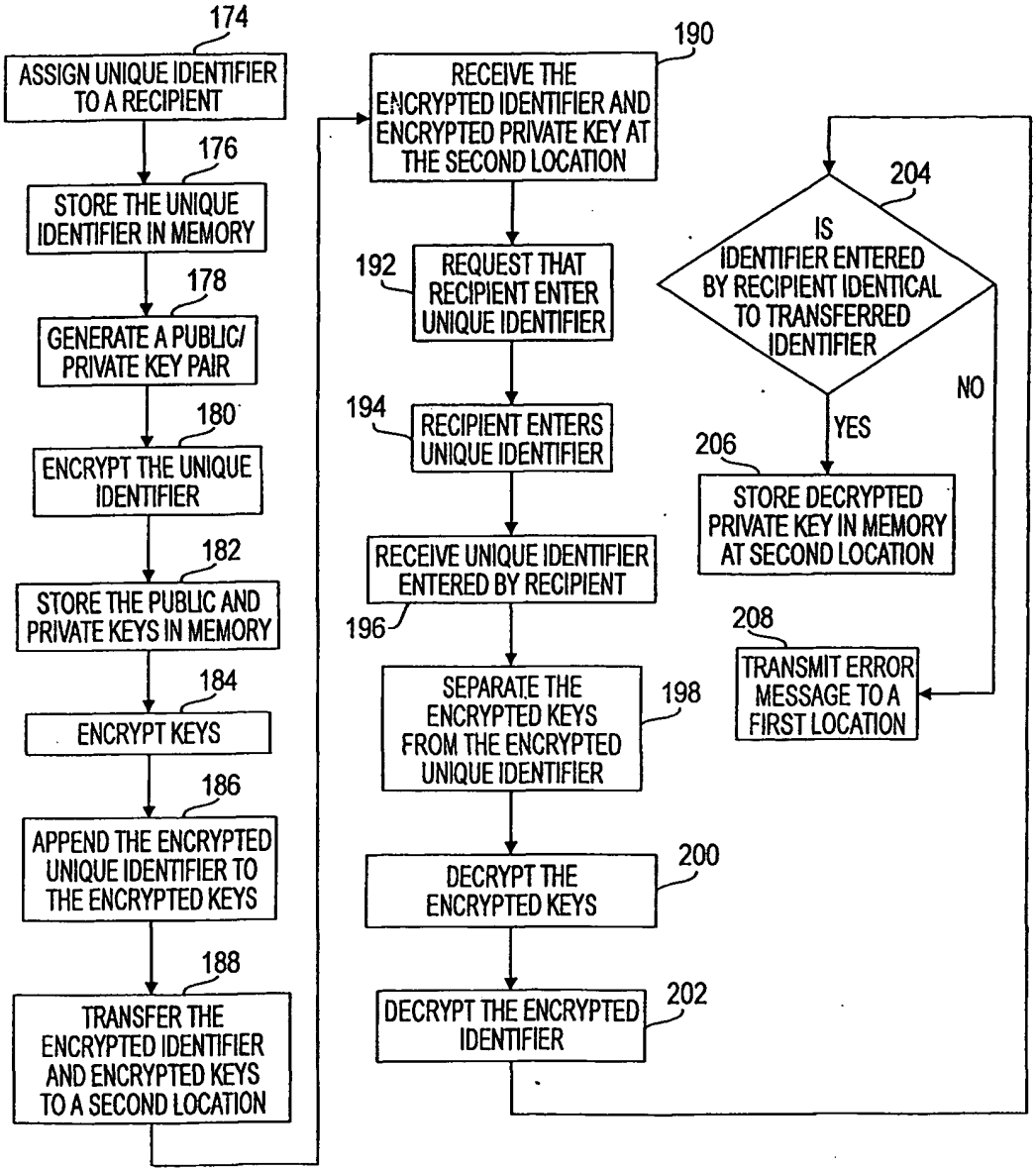

174
ASSIGN UNIQUE IDENTIFIER TO A RECIPIENT
176
STORE THE UNIQUE IDENTIFIER IN MEMORY
178
GENERATE A PUBLIC/ PRIVATE KEY PAIR
180
ENCRYPT THE UNIQUE IDENTIFIER
182
STORE THE PUBLIC AND PRIVATE KEYS IN MEMORY
184
ENCRYPT KEYS
186
APPEND THE ENCRYPTED UNIQUE IDENTIFIER TO THE ENCRYPTED KEYS
188
TRANSFER THE ENCRYPTED IDENTIFIER AND ENCRYPTED KEYS TO A SECOND LOCATION
190
RECEIVE THE ENCRYPTED IDENTIFIER AND ENCRYPTED PRIVATE KEY AT THE SECOND LOCATION
192
REQUEST THAT RECIPIENT ENTER UNIQUE IDENTIFIER
194
RECIPIENT ENTERS UNIQUE IDENTIFIER
RECEIVE UNIQUE IDENTIFIER ENTERED BY RECIPIENT
196
198
SEPARATE THE ENCRYPTED KEYS FROM THE ENCRYPTED UNIQUE IDENTIFIER
200
DECRYPT THE ENCRYPTED KEYS
202
DECRYPT THE ENCRYPTED IDENTIFIER
204
IS IDENTIFIER ENTERED BY RECIPIENT IDENTICAL TO TRANSFERRED IDENTIFIER
NO
YES
206
STORE DECRYPTED PRIVATE KEY IN MEMORY AT SECOND LOCATION
208
TRANSMIT ERROR MESSAGE TO A FIRST LOCATION

FIG. 4

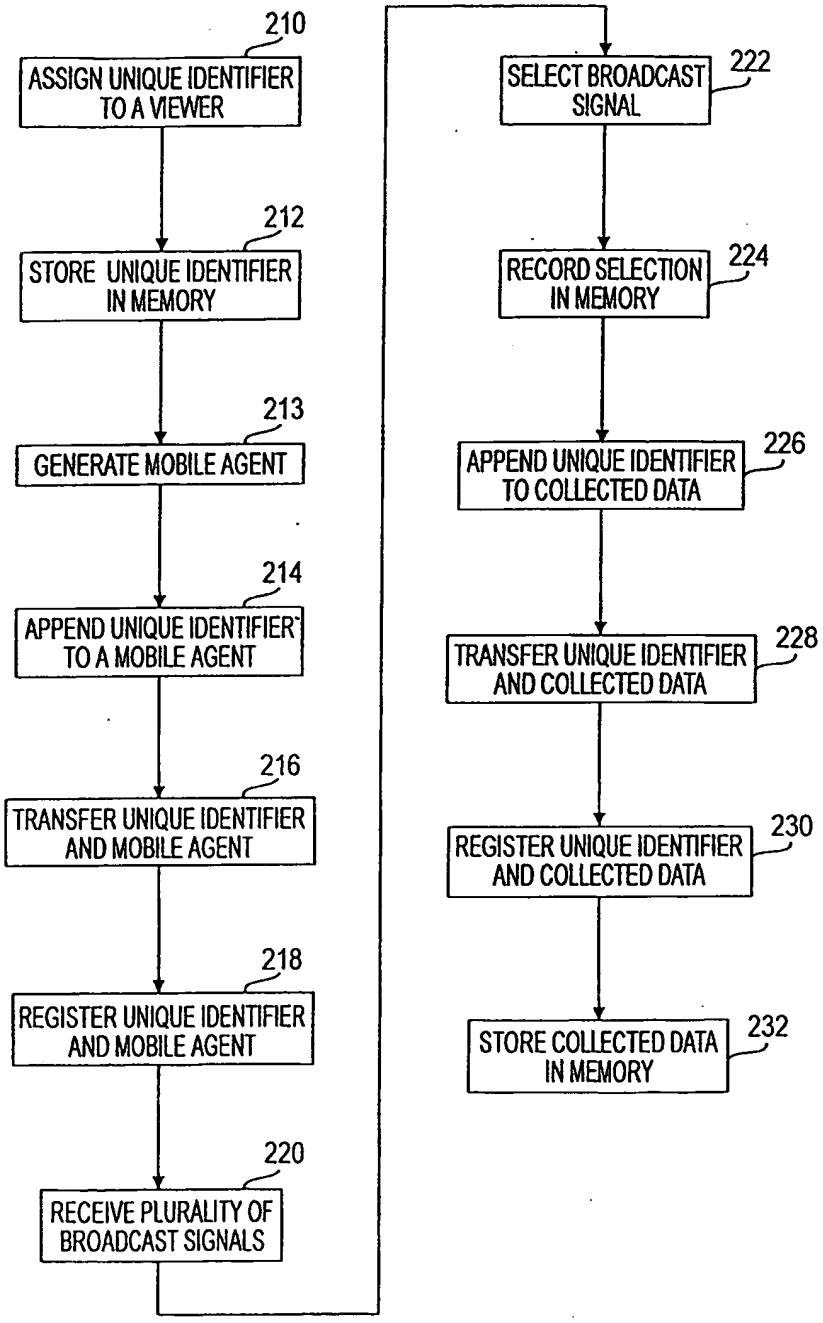

210
ASSIGN UNIQUE IDENTIFIER TO A VIEWER
212
STORE UNIQUE IDENTIFIER IN MEMORY
213
GENERATE MOBILE AGENT
214
APPEND UNIQUE IDENTIFIER TO A MOBILE AGENT
216
TRANSFER UNIQUE IDENTIFIER AND MOBILE AGENT
218
REGISTER UNIQUE IDENTIFIER AND MOBILE AGENT
220
RECEIVE PLURALITY OF BROADCAST SIGNALS
222
SELECT BROADCAST SIGNAL
224
RECORD SELECTION IN MEMORY
226
APPEND UNIQUE IDENTIFIER TO COLLECTED DATA
228
TRANSFER UNIQUE IDENTIFIER AND COLLECTED DATA
230
REGISTER UNIQUE IDENTIFIER AND COLLECTED DATA
232
STORE COLLECTED DATA IN MEMORY

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/33864

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00
US CL : 713/176

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/176, 184,200; 380/230, 231, 232, 233, 282; 705/18, 72

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

IEEE, IBMTDB, DERWINT, EPO, JPO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,160,989 A (HENDRICKS)12 DECEMBER 2000, FIG.s 2, 3, 5, 7, 8, 10a, 10b, 17, col. 9, lines 26-33, col. 10 lines 63-66	33, 35, 36, 37, 63, 64
A	US 6,105,134 A (PINDER ET AL)15 AUGUST 2000, Entire Document	1-76
A	US 5,758,257 A (HERZ ET AL.) 26 MAY 1998, Entire Document	1-76
A	US 5,734,720 A (SALGANICOFF) 31 MARCH 1998, Entire Document	1-76

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 09 APRIL 2001	Date of mailing of the international search report 11 JUL 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harwood PAUL R. CALLAHAN Telephone No. (703) 305-1336

Form PCT/ISA/210 (second sheet) (July 1998) ★